

OFFICE OF CONGRESSIONAL AFFAIRS

Routing Slip

	ACTION	INFO
1. D/OCA		X
2. DD/Legislation		X
3. DD/Senate Affairs		X
4. Ch/Senate Affairs		
5. DD/House Affairs		X
6. Ch/House Affairs		
7. Admin Officer		
8. Executive Officer		X
9. FOIA Officer		
10. Constituent Inquiries Officer		
11.		
12.		

SUSPENSE

Date

Action Officer:

Remarks:

Name/Date



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

O/CONGRESSIONAL AFFAIRS
86-3153

September 17, 1986

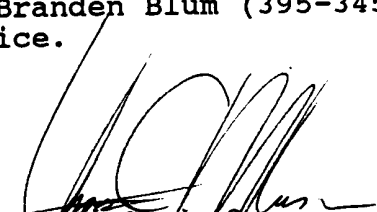
OCA FILE Leo
RECPT # Record

To: SEE ATTACHED DISTRIBUTION LIST

SUBJECT: OMB testimony on S. 2756, the Computer Matching and Privacy Protection Act of 1986.

The attached testimony is provided FYI. No response is required.

Please direct your questions to Branden Blum (395-3454), the legislative attorney in this office.


James C. Murr for
Assistant Director for
Legislative Reference

Enclosure

cc: John Cooney
Frank Seidl
Karen Wilson
Steve Mertens
Alan Rhinesmith

Bob Rideout
Naomi Sweeney
Sara Ducich
Susan Quantius
Suzanne DuVal, w/o attachment
Rob Veeder, w/o attachment

DISTRIBUTION LIST

Department of Agriculture
Department of Commerce
Department of Defense
Department of Education
Department of Energy
Department of Health & Human Services
Department of Housing and Urban Development
Department of the Interior
Department of Justice
Department of Labor
Department of State
Department of Transportation
Department of the Treasury
Environmental Protection Agency
National Aeronautics and Space Administration
Office of Personnel Management
Small Business Administration
United States Postal Service
~~Central Intelligence Agency~~



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

FOR RELEASE ON DELIVERY
Expected at 9:30 a.m.
Tuesday, September 16, 1986

STATEMENT
of
JOSEPH R. WRIGHT, JR.
DEPUTY DIRECTOR
OFFICE OF MANAGEMENT AND BUDGET
Before the
SUBCOMMITTEE ON OVERSIGHT OF GOVERNMENT MANAGEMENT
of the
COMMITTEE ON GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here this morning to discuss S.2756, a bill that seeks to put into statute procedural steps for the use of an important tool in our campaign against waste, fraud and abuse - computer matching. With me is Richard P. Kusserow, the Inspector General of the Department of Health and Human Services and the Vice Chairman of the President's Council on Integrity and Efficiency.

While we have serious concerns about the bill and think that substantial changes are needed to make it workable, it does contain elements of a balanced approach to solving many of the problems related to the use of this technology. On the one hand, it clearly authorizes the government's use of computer matching

by amending the Privacy Act of 1974 to permit disclosures of information for matching purposes. On the other hand, it requires that matching programs include a number of procedural due process steps to preserve the rights of the subjects of any matches.

We certainly support the basic thrust of the bill, especially since it seems to incorporate an approach that we developed years ago and continue to apply in a variety of programs. I want to state at the outset, however, that we do not yet fully understand how the bill's procedures will work in practice, nor exactly what effect they will have on the way our programs are operated; although, later on in this statement, I will point out some areas that we think will be troublesome. As we study the provisions and gather information from the agency program officials and the Inspectors General, we will have a much clearer idea about the kinds of changes that are needed to make the bill work.

Having workable procedures is very important to us because our experience suggests that the imposition of excessive and let me stress the word excessive, administrative procedures will discourage matching. We have found that computer matching is an extremely productive tool in our efforts to prevent, correct and recover erroneous payments in agency programs. Let me give you some idea of the size of the problem we face. While most programs do not measure payment errors, those that do find that

between 4 and 20 percent of all payments go to ineligible persons or constitute overpayments to eligible beneficiaries. In 1984, the Federal share of erroneous payments was about \$900 million in the Food Stamp program, \$500 million in the Medicaid program, and \$485 million in the Aid to Families with Dependent Children program, to take three examples. That is a total of nearly \$2 billion disbursed in error, out of expenditures of about \$42 billion. These erroneous payments are made because of beneficiary errors in reporting income and assets in means-tested programs, use of fraudulent identification documents, and duplicate payments. These errors are of a kind that computer matching is particularly suited to detect and prevent, e.g., in AFDC programs, matching (in conjunction with other management improvements) brought error rates down from 11.1% in 1975 to 6% in 1984. There is simply no way that we could achieve this kind of reduction without resorting to matching. I will give some specific examples later in my testimony.

Moreover, the Congress has demonstrated its understanding of the problem and support for matching by enacting the Debt Collection Act of 1982 as well as the Deficit Reduction Act of 1984.

Provisions in both of these acts work to encourage agencies to reduce error rates and their excessive costs through the use of automated matching. It is important that we not now create unneeded barriers to its use. If we do, the errors will again rise and program costs will increase as we provide services to

those who do not deserve them.

BACKGROUND OF MATCHING

EARLY HISTORY AND DEVELOPMENT OF OMB GUIDELINES

To dispel any concern that matching, as done by the Federal agencies, is taking place in an unregulated environment with inadequate oversight, it is critical to understand how our present procedures came about, the value of matching, and what we are currently doing to guard against misuse of matching.

By 1981, this valuable tool in the fight against fraud, waste and abuse had fallen into unfortunate disuse. To a certain extent, it was a victim of bureaucratic overcautiousness brought about by uncertainty - uncertainty about the effectiveness of matching, about whether the Privacy Act of 1974 permitted the data exchanges necessary to conduct matching programs, and about where the Congress stood on the issue.

But, when computer matching came to the attention of the public in the late 1970s automated auditing was hardly a new process. Agencies had for years been conducting internal financial audits of their programs for quality control purposes. What was new about programs like (then) HEW's Project Match was that their focus on fraud, waste and abuse detection and prevention required the sharing of data across agency boundaries, an activity that

triggered privacy concerns.

We need to remember that the Privacy Act, a statute we are now familiar with, had only been in operation for a few years at that time. Agencies were working to incorporate its principles into their daily operations without a great deal of certain knowledge about its effects on their programs. Little case law had emerged to provide needed interpretations. The only written guidance came from OMB in the form of Implementing Guidelines.

Many agencies at this time were not comfortable with the idea of such data sharing, especially in an automated environment. They remembered that one of the primary forces that brought about the Privacy Act was a concern about the potential effects of automation upon the individual. Indeed, the set of concepts that provided the intellectual foundation of the Privacy Act, the so-called Code of Fair Information Practices, evolved from the work of a 1972 advisory committee on automated personal data systems commissioned by the Department of Health, Education and Welfare. There was a genuine concern, expressed in the preamble to the Privacy Act itself, that the computer had the capability "to greatly magnify" the harm done to the individual. Thus, restrictions on the uncontrolled sharing of personal data among agencies were added to the Act. These restrictions acted as a brake on the development of matching programs, since agencies were not certain that the Privacy Act would support the data

sharing necessary to conduct such programs.

The Privacy Act established as a basic premise the principle that an agency should obtain written consent from a record subject before disclosing his or her records. Recognizing that a totally unthinking adherence to this principle could prevent the government from disclosing when information was necessary to protect the public interest, the Congress wisely wrote into the law a series of narrow exceptions to the written consent requirements. One exception permitted disclosures without consent if they were for a "routine use," and it was under this exception that most data transfers for matching purposes took place. This exception in the Privacy Act defined a "routine use" as a use that was compatible with the purpose for which the agency originally collected the data. The vagueness of the term was offset by a requirement that agencies publish their proposed routine uses in the Federal Register where they would be subject to public scrutiny and comment.

While compatibility was the standard that controlled disclosure, it was not defined in the Act; nor, as I noted earlier, was case law at this time at all developed on the issue. Thus, early in the agencies' implementation of the Privacy Act, concerns over whether compatibility could truly be demonstrated caused some agencies to decline to participate in several matching programs.

It was clear that standards for matching programs were needed, and in 1979, in an effort to bring procedural consistency to the agencies' use of matching, and to enforce a discipline on the process, OMB issued "Guidelines on the Conduct of Computer Matching Programs." The effect of these Guidelines was to legitimize matching if it took place within the provisions of the Privacy Act but to disallow it otherwise. The Guidelines provided rules that the agencies found useful in implementing matching programs. Moreover, Congress itself looked on the 1979 Guidelines as providing a needed procedural structure in which matching could take place. The legislative history of the Inspector General Act of 1978 shows that the drafters expected that OMB's proposed "Matching Guidelines" would be followed by the new Inspectors General in conducting any matching programs in order to ensure a "useful balancing of the competing values [protection of privacy vs. governmental efficiency]....Matching programs will occur, but only in conformity with the protections contemplated by the Privacy Act."

The Matching Guidelines were designed with two basic goals in mind:

- o To require that the agencies themselves, the public, the central management agencies and the Congress understand and evaluate matching programs before they took place; and

- o To create a uniform set of procedures for agencies to follow in conducting matching programs that would ensure that agencies conformed to Privacy Act requirements for data sharing.

The oversight procedures consisted essentially of publication and reporting provisions. Agencies were required to publish notices describing proposed matching programs as well as any routine uses associated with these programs to solicit public comment. They were also required to report matching programs to OMB and the Congress 60 days in advance of their implementation.

The uniform procedures covered both interagency matches as well as intra-agency matches to combat fraud, waste and abuse. However, matches for administrative or statistical purposes were not covered. The procedural steps took agencies through the process of determining whether to do a match; and if so, how to do it. The preliminary step required the agency to complete a benefit/cost analysis that included an analysis of alternatives to matching and an explanation of why the alternatives were not chosen. In the remaining steps, the agency was required to define the data to be used, prepare the Federal Register notices for new systems or routine uses, and finally terminate the match and dispose of the materials used. "Source" agencies were cautioned to review material they were asked to provide to the agency performing the match to determine the appropriateness of

the matching program. Sources were also cautioned to have in place the appropriate Privacy Act systems of records and routine uses before participating in any matching program.

During the 3 years that these Guidelines were in effect, OMB received 20 matching reports. The Departments of Agriculture and Health and Human Services submitted 75% of the reports, most of which reported programs designed to uncover fraud and abuse in Food Stamp and Aid to Families with Dependent Children programs. Indeed, a follow-on to HHS's "Project Match" which was the progenitor of modern matching programs was among these. The Department of Education and the Veterans Administration accounted for the remaining 25%.

Because the Guidelines were new and their procedures untested, OMB staff spent a great deal of time in contact with agency personnel working out the details of what was needed to comply with both the Matching Guidelines and the Privacy Act. The ultimate agency report to OMB and the Congress was simply the documentation of that close coordination. In no case did OMB review of these reports reveal any violation of either the Privacy Act or the Matching Guidelines because great care was taken before hand to make sure a violation did not exist.

Moreover, these Guidelines appeared to have satisfied both Congressional and public concerns over matching. Few public

comments were ever generated by agency publication of proposed matches; comments that were received raised no substantive concerns.

The Guidelines, while allaying to a certain extent, agencies' concerns about the legality of matching, had their own problems. They were unnecessarily expensive and administratively difficult for agencies to implement. They were hard to understand. Moreover, despite reassurances, some agencies remained concerned about the propriety of this kind of data sharing and were reluctant to participate in broad-based interagency matching programs. Thus, after a promising beginning, computer matching of the Project Match variety gradually faded away and languished until the early 1980's.

EFFORTS OF THE PRESIDENT'S COUNCIL ON INTEGRITY AND

EFFICIENCY TO REVITALIZE MATCHING

This Administration recognized the value of this tool very early. In March of 1981, President Reagan established the President's Council on Integrity and Efficiency (PCIE), an organization that took the lead in revitalizing matching to fight waste, fraud and abuse. Composed of the statutory Inspectors General and representatives of other major Federal executive agencies, the new Council immediately began to consider major initiatives to

fulfill the President's Executive Order. It is a group which I chair.

As a result, in the past 6 years, matching has evolved from a somewhat controversial and misunderstood process into a mature and rather routine albeit very successful one.

One of the first major projects the PCIE undertook was the Long Term Computer Matching project, co-chaired by the Inspectors General of the Department of Health and Human Services and the Department of Labor. Dick Kusserow, the Vice-Chairman of the PCIE, personally took the lead in that project. The major goal of this project was to promote the cost-effective use of computer matching to combat fraud, abuse and erroneous payments in federally funded programs. Through its membership of Federal and State program administrators, the project sought to:

- o gather and share information about Federal and State matching activities;
- o identify and remove technical and administrative obstacles to computer matching, while preserving essential protections and safeguards to personal data; and
- o foster increased Federal and State cooperation in computer matching activities.

One of the project's first tasks was to recommend ways to improve the OMB "Guidelines for Conducting Computer Matching Programs;" to streamline the paperwork requirements while preserving the requirements for privacy and security of records. The revised guidelines, issued on May 11, 1982, incorporated many agency recommendations for clarification and change based on their actual operating experiences. While streamlining the paperwork requirements for justification and approval, the revised guidelines preserve the requirements for Federal Register notices and strict safeguards concerning use, storage, and disclosure of information from matches.

As further guidance to agencies in complying with the Privacy Act and the 1982 Guidelines, the PCIE developed a "Model Control Systems and Resource Document for Conducting Matching Projects Involving Individual Privacy Data." This document provides an approach to conducting computer matching that meets the requirements of the OMB Matching Guidelines. Specifically, it provides a methodology for assuring adequate protection of personal data during computer matching and presents a model set of processes and procedures for use when undertaking computer matches.

On December 29, 1983, OMB issued to all Federal executive agencies this document and the "Computer Match Checklist" which

is to be completed by each agency engaging in or providing data for computer matching of Federal, State or local entities. The checklist was designed to ensure documentation of compliance with Privacy Act and OMB Matching Guidelines. The checklist must be completed and maintained for use in annual submissions to OMB under reporting requirements of the Privacy Act, as well as for review by OMB, GAO or others to ensure safeguarding and prudent management decisions regarding matching.

The PCIE Long Term Computer Matching Project has also done much to advance the cost-effective use of computer matching techniques in detecting errors and verifying eligibility for government programs. For example, the project included a catalogue of both State and Federal use of computer matching and related techniques, including State use of front-end verification techniques. These inventories served to document the extent of matching at the time and to heighten awareness to the array of possible applications of the technique.

There are additional examples of what the Long Term Computer Matching Project has done to promote efficient and secure matches.

- o The Computer Matching Newsletter is a quarterly publication designed to promote the sharing of computer matching technology and applications among Federal and State agencies.

- o The Standardized Formats, developed to facilitate State computer matches, created standardized data elements and record formats. These are now being used in the implementation of the 1984 Deficit Reduction Act requirements, which I will discuss later.
- o The Manager's Guide to Computer Matching, which contains a methodology for cost and benefit analysis, provides managers of State benefit programs with a practical guide to conducting matches.
- o Project Clean Data is a computer program that can be used by Federal, State and local agencies to increase the integrity of personal files by identifying incorrect or bogus Social Security numbers.

Beyond the issue of safeguarding personal data in the conduct of computer matches, the PCIE is also sensitive to the security of computer systems. So, in 1981, the Computer Security Project was initiated and has operated in tandem with the Long Term Computer Matching Project. The major goals of the Computer Security Project were to document known cases of computer-related fraud and abuse, identify common vulnerabilities, and develop methods to assure the integrity of Federal information systems and State systems administering Federal programs.

One of its first initiatives was a two part study of computer-related fraud and abuse. Initially all Inspectors General were surveyed to identify all known cases of fraud and abuse that involved government computers. Beyond identifying 69 fraud and 193 abuse cases, the survey was able to document a number of generic vulnerabilities in government computer systems. The second phase of the study involved the interviewing of 46 perpetrators of computer related fraud. Those interviews provided new insights in the who, how, and why of these crimes.

The PCIE has also studied the integrity of electronic media billing, and conducted a security seminar for Inspectors General and Assistant Secretaries for Management. In the coming fiscal year it will initiate studies to assess computer security in State agencies administering Federal benefit programs, improve the auditability of computer systems, and survey system life-cycle integrity and control requirements.

CURRENT SUCCESSFUL MATCHING PROGRAMS

Since 1981, the way in which the PCIE and the agencies use computer matching has matured. Agencies appear to be careful to assess the cost-effective potential of matches and to follow the procedural requirements. It is important to emphasize that we have had no evidence of any Federal abuses in computer matches

and in the many Federal and State applications of matching, many substantial savings are evident. For example:

- o The State of New York routinely matches welfare recipient records with quarterly wage reports and has estimated over a 300 percent return on the costs of this system.
- o The Social Security Administration routinely matches its Supplemental Security Income files against the Veterans Administration's compensation and pension files, saving millions in erroneous payments and costly manual verifications.
- o In 1982, the Department of Education ran lists of delinquent student loan debtors against Federal employee active and retired rolls and recovered \$3.4 million.
- o In 1985, Social Security files were matched with OPM pension files which identified individuals receiving payments from both systems without the proper offsets will result in \$41 million in cost avoidances.
- o In October 1985, the State of Missouri matched SSI data with Medicaid files to identify individuals who were residing in Medicaid reimbursed facilities but receiving full SSI payments. The match identified over \$44,000 in overpayments

while costing only \$10,000 to run.

- o In July 1985 the records of four million SSI recipients were matched with IRS unearned income files (Form 1099). This match identified \$117.5 million in overpayments for which recovery action was instituted. The full cost of conducting the match, including the cost of follow-up, is \$6.4 million.

Certainly this array, and the many other examples, of successful matching projects helps to demonstrate the value of matching. The Congress apparently agrees and has demonstrated its support for the use of this technology in such legislation as:

- o The Debt Collection Act of 1982 authorized several important applications for computer matching. Applicants for loan assistance were required to provide their taxpayer identification numbers (Social Security Account Number (SSN) for individuals) which enabled agencies to screen loan applicants or recipients against IRS delinquent tax files. Federal employee SSNs can be matched against the delinquent debt files of other Federal credit agencies. In addition, the Debt Collection Act authorized the IRS to release to Federal agencies the addresses of delinquent debtors to be used in collection efforts.
- o The Tax Equity and Fiscal Reliability Act of 1982, in which

Congress set statutory targets for States to meet in reducing errors in public assistance programs -- 3% for AFDC and Medicaid by 1984. The Food Stamps Amendments of 1982 set a target of 5% for Food Stamps for 1985. All three programs were given interim targets beginning in 1980. Congress reacted to a lack of progress in meeting these targets by passing the income and eligibility verification provisions of the Deficit Reduction Act of 1984 (DEFRA).

- o The Income and Eligibility Verification provisions of the 1984 Deficit Reduction Act. In proposing this legislation, the Congressional intent was to reduce erroneous payments in federally funded benefit programs. This legislation authorized the Social Security Administration's Supplemental Security Income (SSI) program and State agencies administering the Aid to Families with Dependent Children (AFDC), Food Stamps, and Medicaid programs to request and use data from IRS on unearned income (interest, dividends, etc.) in determining individuals' eligibility for assistance. DEFRA also reaffirmed and strengthened existing authority for AFDC and Food Stamps to use wage data from the Social Security Administration and from State Employment Security Agencies. It is important to note that underlying these data exchanges, the DEFRA provided specific protections against misuse, such as safeguarding requirements, notice of use of data, and independent verification of the IRS unearned income data. In

a typical match, each month the States send their computer tapes, with records on individuals who have applied for AFDC, Medicaid, and Food Stamps in the prior month, to IRS to be matched against the IRS unearned income file. In the aggregate, this would result in about 250,000 records on public assistance applicants being matched against a file containing records on nearly 180 million individuals' unearned income like interest and dividends payments reported to IRS by financial institutions. Similar matching takes place at SSA. Although this process is too new to allow us to report quantified results, the Congressional Budget Office, prior to DEFRA passage, estimated that DEFRA matching programs would save \$275 million in 1987.

We anticipate that as the Congress sees that matching programs like these are cost effective and are being conducted with due regard to the rights of those involved, it will consider other benefit programs for inclusion.

For our part, we will be proposing that a number of programs be allowed access to wage and unearned income data, Social Security and unemployment compensation data. These programs include veterans benefits and medical care, means-tested housing programs, child nutrition programs, maternal and child health block grants, student aid programs, health education assistance and health professions and nursing student loans, railroad

retirement, Federal Employees Compensation Act, and civil service disability retirement. Such an expansion of current coverage would, of course, include privacy and due process protections at least as comprehensive as those in DEFRA.

I think my testimony thus far has demonstrated why we think matching is such an important and useful tool and what we are doing to ensure that it is conducted in a way which comports with existing statutory protections such as the Privacy Act. I would like to turn now to a discussion of some of the specific provisions of S. 2756 and point out some of the troubling procedural problems our initial analysis has revealed.

ANALYSIS OF S. 2756 PROVISIONS AND COMMENTS

As I said earlier, we see S. 2756 as having two main goals:

- o It seeks to establish uniform procedures under which agencies would perform matches so that the subjects of the matches are afforded due process;
- o It seeks to establish a number of oversight mechanisms to ensure that agencies implement the bill's procedures.

Many of the provisions of the bill are drawn from existing OMB issuances, e.g., Guidelines on the Conduct of Matching Programs

and Appendix I to OMB Circular No. A-130. While we would prefer to see them remain exclusively in regulation so that they can be more readily altered to fit changing circumstances, we think they are fundamentally sound and have no objection to their inclusion in this bill.

There are some new provisions, however, that we think may have negative consequences that the Congress did not intend:

- o Section 2(b)(3) of the bill requires that matching agreements contain an assurance that "individuals whose records are matched will be notified of such matching program or front-end eligibility verification program and the procedures for providing such notice...."

While we agree that individuals should be made aware of the uses of data they provide or data that is about them, we are concerned about the breath of this requirement. Read literally, it would mean that each time an agency wished to conduct a matching program, it would have to write to each individual whose records were involved. It would have to do so on a continuing basis, for example, for eligibility-for-benefits verifications even when the applicant had been advised that such checks would occur annually for as long as he received benefits. Such a procedure would turn matching from a relatively simple verification process to an

ineffective and prohibitively expensive one. Few agencies would be able to use it. Let me give you some examples to illustrate the scope of this problem:

- Currently, neither the Internal Revenue Service nor State tax agencies issue notices to individuals affected by matches conducted for tax compliance purposes under the Federal/State Exchange Program. If the Service were required to issue such notices, almost every taxpayer in the country would have to receive one or more. The postage alone would likely approach \$20 million.
- The SSI/VA match I cited earlier is designed to determine if any SSI beneficiaries are receiving benefits from the Veterans Administration that would affect the level of SSI benefits. This match is run six times each year and involves nearly 10 million individuals' records. VA estimates that postage alone for these six matches would total \$10 million. Note that this figure does not include preparation and processing time for the notices. That is a significant amount of money to charge off to operating costs.
- State Child Support Enforcement agencies routinely match files of absent parents with Federal, State and local files in order to locate parents who are not meeting their

obligations to support their dependent children, many of whom are on welfare. In locator matches like these, it would be literally impossible to comply with a specific notice requirement, since the point of the match is to develop address information.

-- In matches done to uncover evidence of fraudulent behavior, such as HHS matches designed to uncover physicians who are double-billing Medicare and Medicaid for the same service, providing notice would alert those being investigated and permit them to alter their behavior long enough to avoid detection.

Moreover, what good does it do an individual to know that an agency intends to match data about him after he has provided the data? Such notice occurs at the wrong point in the process. The proper point is when he is about to provide the data and has the ability to decide not to, and Section (e)(3) of the Privacy Act already requires that individuals receive notice at this point. Admittedly, such notice is often fairly general, e.g., "we intend to check other data sources to verify the information in your application," but it does occur at the right time. It also serves a deterrent purpose by making an applicant think twice about supplying false data.

As to specific matching programs, our current practice is to

publish a notice in the Federal Register. I understand that the Federal Register is not the most widely read journal; but it is essentially the "house organ" of the government and the place where we can put a more complete description of a matching program than can occur on an application form.

Once the match has occurred and reveals adverse data, the follow-up investigative process inevitably involves providing the individual notice.

We think the procedures we are currently using achieve the notice that the bill aims at in a way that allows matching programs to be operated efficiently and at the same time preserves the privacy rights of the individual. Anything more would probably be unnecessary overkill and we recommend that the wording of the section be amended to make it clear that general notice of specific matches would constitute the kind of notice that the bill calls for. For our part, we will ensure that application forms used by the Federal agencies will be scrutinized for the adequacy of their Privacy Act notices. And, as you know, under the Paperwork Reduction Act, all of these forms must be approved in advance by OMB.

- o Section 3 of the bill amends the Privacy Act to require publication of notices of matching programs in the Federal Register 30 days prior to their initiation. It also amends

the Privacy Act to put reports on matching programs in the same reporting category as reports on new Privacy Act systems of records.

We would urge that the provision be amended to permit OMB to waive the publication and review time period if the agency can demonstrate that public harm will result from a delay in conducting the match.

- o Section 4 of the bill requires that agencies establish Data Integrity Boards to approve matching programs and to carry out some of the review requirements of OMB Circular No. A-130. Since the IG is not a statutory member of this group, this provision would unwisely conflict with his independence and authorities. Moreover, it is not clear that adding another bureaucratic layer to agency level oversight is appropriate.

Instead, we would like to propose an administrative solution that goes somewhat beyond the statutory proposal. Two OMB regulations, OMB Circular Nos. A-123 and A-130 already address aspects of the oversight problem. A-123 charges agency managers to work actively to prevent fraud and waste and to implement the requirements of the Federal Managers' Financial Integrity Act of 1982 (31 U.S.C. 3512), especially as related to conducting reviews to uncover weaknesses in internal management control and accounting systems. The Circular

requires two kinds of reviews:

- The first assesses the risk of fraud, waste and abuse, as well as other losses in program and administrative activities.
- The other requires a more detailed review of higher risk areas to find out if needed controls are in place and working.

Reports to the President and Congress are made annually as to whether agency heads have reasonable assurance that controls are in place and working and that list material weaknesses in the controls.

When I sent the circular to the agencies in August, I asked them to "place a particular emphasis in the next few years on preventing unauthorized use of confidential information -- of both manual and automated files and telecommunications. Maintaining privacy for U.S. citizens is an important goal of this Administration."

OMB Circular No. 130 works with A-123. It states the government's policy on information and the technology associated with its creation, maintenance, use and disposition. Appendix I of this Circular contains

requirements for agencies' compliance with the Privacy Act, including requirements for many of the reviews that the bill also requires the Data Integrity Boards to conduct.

It is clear to me the two Circulars working together embody the elements of such Data Integrity Boards. Indeed, together they add up to a much more comprehensive review and and reporting arrangement than the bill proposes and one that would have a large privacy dimension. What we need to do, and what I propose that we do, is to better integrate these two regulations and develop a much broader based activity within the agencies than one that is concerned only with computer matching. We intend to incorporate the results of this activity into our annual report to Congress.

- o Section 5 of the bill deals with the important subject of verification of data. We strongly support the goal of this section -- to ensure fair treatment of individuals affected by computer matches. In fact, virtually all Federal programs currently afford similar protections, not only in computer matching situations but in all circumstances where individual eligibility for benefits is in question, regardless of the source of information. This duplication of requirements between existing statutes, regulations, and case law is of concern to us because it has the potential to cause conflict and confusion in program operations.

In a typical federally-funded benefit program, client circumstances change frequently and information flows to caseworkers from many sources -- the clients, other programs, State and local agencies, as well as through computer matching programs with Federal sources. These programs routinely verify the information, provide an opportunity to refute, and give notice of an adverse action and right to hearing. A separate requirement, as proposed by this bill, would burden caseworkers with tracking the source of information in case files so that they could comply with two sets of due process rules. To avoid this, we would recommend that the bill affirmatively state what should constitute the minimum protections applicable to all programs, without attempting to write any specifically into law.

We would also point out that the requirement that all information be independently verified, through either the affected individual or a third party, may cause some operational problems. For example, Social Security Administration data on Social Security benefits cannot be independently verified by any third party; an agency using this information would be compelled to verify it by contacting the recipient and this could jeopardize an agency investigation in a criminal case. We recommend that the

bill requirement for independent verification be modified to permit agencies to use the data without independent verification in limited situations.

- o Section 2(a) of the bill adds a new disclosure exception to the Privacy Act to authorize data sharing without the consent of the record subject when it is done pursuant to a "matching agreement," the terms of which are defined in Section 2(b) of the bill.

While we think that it will be useful to have such a disclosure exception, we think the provision as proposed is overly broad. It will bring within its scope matches that we do not think the drafters intended to cover. Two specific examples come to mind:

- Matches on individuals made for law enforcement purposes - from systems like the National Driver Register, for example.
- Internal agency matches for administrative purposes when the "hits" are disclosed outside the agency - for overtime payment, for example.

In each of these cases, (b)(12) would require that the matching agency go through all the agreement, notice and due

process steps. We do not think that this is what the drafters intended. We suggest, therefore, that the provision be redrafted to cover only a more narrow category of matching programs.

I want to emphasize that these concerns I've expressed relate primarily to how the bill's provisions would actually be implemented. But, we will have to deal with these concerns effectively if we are to avoid unwarranted damage to an important tool in all of our efforts to reduce fraud, waste and abuse. Again, let me say that we are in agreement about the bill's underlying goal: to improve the efficiency of governmental programs while protecting the privacy rights of our citizens. We look forward to working with you in this important endeavor.

This concludes my statement. I'll take any questions you have.